

5 THINGS RANSOMWARE AND DDoS ATTACKS HAVE IN COMMON

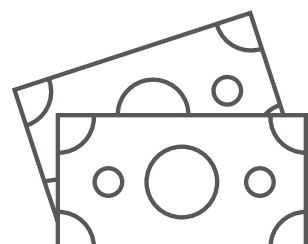
But It's the One Thing They Don't Have in Common That Can Hurt You

1 FINANCIAL MOTIVATION



RANSOMWARE

"Pay me for the decryption key to unlock your files"



DDoS EXTORTION

"Pay me or I'll launch another DDoS attack to bring down your network/services"



RANSOMWARE

Ransomware incidents have accounted for 41% of cyber insurance claims filed in the first half of 2020.

2 UPWARD TREND IN 2020

Especially during COVID-19 Pandemic

DDoS EXTORTION

In 1H 2020 we have seen 4.8 Million DDoS attacks, a 15% YOY 1H 2020 Threat Report.

3



MITRE ATT&CK®
IMPACT = AVAILABILITY
A form of Denial of Service (DoS)

RANSOMWARE

Encrypt data to interrupt availability to system and network resources.

DDoS EXTORTION

Degrade or block the availability of services or resources to users.

4 READILY AVAILABLE ATTACK TOOLKITS

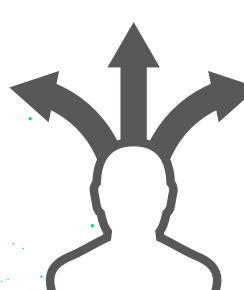
RANSOMWARE

Common ransomware tools include affiliate programs that adversaries can easily buy and obtain multiple ransomware malware families



DDoS EXTORTION

Common DDoS attack tools DDoS-for-Hire and Booter/Stresser Services are readily available and very inexpensive.



RANSOMWARE

Lack of data backups, network segmentation, and recovery programs.

5 ATTACKERS TAKE ADVANTAGE OF TARGET'S UNPREPAREDNESS

DDoS EXTORTION

Lack of adequate DDoS protection and plan

Which brings us to the one way ransomware and DDoS are different.

ABILITY TO CONTROL FATE



RANSOMWARE

No

Pay the attackers and trust they will provide the decryption key.

DDoS EXTORTION

Yes

Plenty of DDoS attack protection products and services.

NETSCOUT's Arbor Edge Defense can be a First and Last line of Perimeter Defense to stop DDoS attacks and the download of ransomware before encryption occurs.

netscout.com/product/netscout-aed